

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, S.S.

**SUPERIOR COURT
BUSINESS LITIGATION SESSION**

JANE DOE, JOHN DOE, JAN DOE,
JAMES DOE, AND JANET DOE,
INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

C.A. No. 2384CV01236-BLS1

Plaintiffs

V.

CAPE COD HEALTHCARE, INC.,

Defendant.

**FIRST AMENDED CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

| | |
|--|----|
| NATURE OF ACTION AND ALLEGATIONS..... | 1 |
| PARTIES TO THE ACTION | 2 |
| JURISDICTION AND VENUE | 3 |
| FACTUAL BACKGROUND..... | 3 |
| A. Plaintiffs' experience with Defendant. | 3 |
| B. Defendant routinely disclosed the protected health information of its patients to third parties including Facebook and Google..... | 5 |
| C. Defendant misuses sophisticated software to automatically collect and disclose patient PII/PHI to third-party advertising companies like Google and Facebook..... | 6 |
| D. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website..... | 12 |
| E. Facebook's Business Model: Exploiting Users' Personal Information for Profit. | 18 |
| F. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites..... | 21 |
| G. Defendant has discretely embedded the Meta Pixel tool on its website, capturing and disclosing patients' PII/PHI to Facebook. | 27 |
| H. Plaintiffs and the Class Members did not consent to the interception and disclosure of their protected health information..... | 38 |
| I. The disclosures of personal patient data to Facebook are unnecessary..... | 41 |
| J. Plaintiffs and Class Members have a reasonable expectation of privacy in their PII/PHI, especially with respect to sensitive medical information. | 41 |
| K. Defendant harmed Plaintiffs when it illicitly collected, disclosed, and exploited Plaintiffs' PII/PHI—which, after all, is Plaintiffs' property, and has economic value. | 44 |
| L. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' PII/PHI..... | 46 |
| TOLLING, CONCEALMENT, AND ESTOPPEL..... | 46 |
| CLASS ACTION ALLEGATIONS | 47 |
| CAUSES OF ACTION | 51 |
| COUNT I | 51 |
| Interception of Wire Communications in Violation of | 51 |

| | |
|--|----|
| 18 U.S.C. § 2510, <i>et seq.</i> | 51 |
| (On Behalf of Plaintiffs and the Nationwide Class) | 51 |
| COUNT II | 56 |
| Invasion of Privacy in Violation of G.L. c. 214, § 1B | 56 |
| (On Behalf of Plaintiffs and the Massachusetts Class) | 56 |
| COUNT III | 59 |
| Breach of Fiduciary Duty and/or Common Law Duty of Confidentiality | 59 |
| (On Behalf of Plaintiffs and the Massachusetts Class) | 59 |
| COUNT IV | 60 |
| Breach of Implied Contract | 60 |
| (On Behalf of Plaintiffs and the Massachusetts Class) | 60 |
| COUNT V | 69 |
| Unjust Enrichment | 69 |
| (On Behalf of Plaintiffs and the Massachusetts Class) | 69 |
| DEMAND FOR JURY TRIAL | 70 |
| PRAYER FOR RELIEF | 70 |

Plaintiffs Jane Doe, John Doe, Jan Doe, James Doe, and Janet Doe (“Plaintiffs”), individually and on behalf of all other persons similarly situated (“Class Members”), bring suit against Defendant Cape Cod Healthcare, Inc. d/b/a Cape Cod Hospital, Falmouth Hospital, and JML Care Center (“Defendant” or “Cape Cod Healthcare”), and upon personal knowledge as to Plaintiffs’ own conduct and on information and belief as to all other matters based upon investigation by counsel, allege as follows:

NATURE OF ACTION AND ALLEGATIONS

1. This case arises from Defendant’s systematic violation of the medical privacy rights of its patients, exposing highly sensitive personal information to third parties without those patients’ knowledge or consent.

2. Defendant’s “Privacy Policy” assures patients that “[a]t Cape Cod Healthcare, we are committed to protecting the privacy and security of the users of our internet site.”¹ Indeed, Defendant promises patients that it is “committed to protecting the identities of visitors to our site” and that, other than disclosing personal information to process credit card information, it ‘has no other current plans to make other disclosures of such information.’² Contrary to these assurances, Defendant does not follow these policies, nor the law prohibiting such disclosures.

3. At all relevant times, Defendant disclosed information about its patients—including their status as patients, their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Facebook and other third parties without their patients’ knowledge, authorization, or consent.

4. Defendant discloses this protected health information through the deployment of various digital marketing and automatic rerouting tools embedded on its websites that purposefully and intentionally redirect patients’ personal health information to third parties who

¹ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

² <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

exploit that information for advertising purposes. Defendant's use of these rerouting tools causes its patients' personally identifiable information and the contents of its patients' communications exchanged with Defendant to be automatically redirected to third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, and both the express and implied promises of Defendant.

5. Defendant's conduct in disclosing such protected health information about its patients to Facebook and other third parties violates both Massachusetts and Federal law.

PARTIES TO THE ACTION

6. Defendant Cape Cod Healthcare, Inc. is a Massachusetts corporation with its principal office at 27 Park Street, Hyannis, MA 02601. Defendant is a private health system providing healthcare services for residents and visitors of Cape Cod.³ Defendant owns and manages numerous healthcare facilities in Massachusetts, including Cape Cod Hospital, Falmouth Hospital, JML Health Care Center, Cape Cod Surgery Center, Davenport-Mugar Cancer Center, Falmouth Hospital Rehabilitation Center, Cape Cod Healthcare Urgent Care-Falmouth, Cape Cod Healthcare Urgent Care-Harwich, and Cape Cod Healthcare Pharmacy.⁴

7. Plaintiff, Jane Doe has a residence in Barnstable County, Massachusetts, has been treated by Defendant's physicians, and has been a patient of Defendant.⁵

8. Plaintiff John Doe has a residence in Barnstable County, Massachusetts, has been treated by Defendant's physicians, and has been a patient of Defendant.

9. Plaintiff Jan Doe has a residence in Barnstable County, Massachusetts, has been treated by Defendant's physicians, and has been a patient of Defendant.

³ <https://www.capecodhealth.org/about/>

⁴ <https://www.capecodhealth.org/locations/>

⁵ <https://www.capecodhealth.org/locations/profile/cape-cod-hospital/?searchId=db38b971-ab75-ed11-a85a-000d3a611c21&sort=11&page=1&pageSize=10>

10. Plaintiff James Doe has a residence in Barnstable County Massachusetts, has been treated by Defendant's physicians, and has been a patient of Defendant.

11. Plaintiff Janet Doe has a residence in Barnstable County, Massachusetts, has been treated by Defendant's physicians, and has been a patient of Defendant.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Massachusetts and has its principal place of business at 27 Park Street, Hyannis, Massachusetts, 02601. G.L. c. 223A, § 2; G.L. c. 223A, § 3.

13. Venue is appropriate in this Court because Defendant resides in Barnstable County and the acts or conduct giving rise to the cause of action took place in Barnstable County. G.L. c. 223, § 1.

FACTUAL BACKGROUND

A. Plaintiffs' experience with Defendant.

14. Plaintiff Jane Doe is a patient of Defendant who has received treatment from Defendant at Cape Cod Hospital.⁶ Since at least 2021, Plaintiff Jane Doe visited Defendant's website at www.capecodhealth.org regularly to search for a doctor and look up treatments for her medical conditions. Among other things, she has used Defendant's Website to research MOHS surgery for skin cancer. She has also used Defendant's patient portal to review test results, including x-rays and ultrasounds, review summaries of visits from her doctor, and check referrals. When doing so, she entered identifying information and information related to her medical condition and doctor, including queries about treatment for skin cancer.

15. Plaintiff John Doe has been using Defendant's patient portal consistently for approximately the past six years. He has used it to check medications, pay bills, and check labs

⁶ <https://www.capecodhealth.org/locations/profile/cape-cod-hospital/?searchId=db38b971-ab75-ed11-a85a-000d3a611c21&sort=11&page=1&pageSize=10>

and other results. Such activities related to his treatments for knee surgery and to have a stent put in his heart. When doing so, he entered identifying information and information related to his medical condition and doctor, including queries about his heart-related health issues.

16. Plaintiff Jan Doe has also been using Defendant's website and accessing Defendant's patient portal for several years. She used the website to find providers, schedule appointments, pay for medical services, and research treatments. Specifically, she researched weight loss drugs, knee replacement recovery, and mammograms. She would use the patient portal to check lab results for biopsies and bone density tests. When doing so, she entered identifying information and information related to her medical condition and doctor, including queries about knee replacement surgeries and recovery. After using Defendant's Website and patient portal she noticed online advertisements related to weight loss and knee replacement-related pain.

17. Plaintiff James Doe similarly used Defendant's website over the past several years to research treatments available from Defendant, including through his PCP and cardiologist. He has also used the patient portal regularly in the past several years to follow up on treatment he received from Defendant. Among other things, he used the portal to review information about tests that he underwent at Cape Cod Hospital for his heart condition. When doing so, he entered identifying information and information related to his medical condition and doctor, including queries about his heart condition.

18. Plaintiff Janet Doe has been using Defendant's website for at least the past seven years. She has used it to find new providers, to search for medications, to learn more about COVID-19, to book appointments, and to research gastroenterology and dermatological conditions. She further used the patient portal for tasks including looking at test results and labs and making appointments. When doing so, she entered identifying information and information

related to her medical condition and doctor, including queries about her dermatological and gastroenterological conditions.

19. Plaintiffs all believed that their interactions with Defendant's website were private and would not be shared with anyone besides her health care providers and their staff. None of them consented to Defendant sharing any information about their use of the Website or the patient portal with Facebook, Google, or any other third party. Unbeknownst to Plaintiffs, Defendant installed tracking technologies across its webpages that caused the medical information Plaintiffs entered on those webpages, their personally identifiable information including their IP Addresses and Brower Fingerprints, and Plaintiffs' interactions with Defendant's webpages, to be transmitted to third party advertisers without their consent.

B. Defendant routinely disclosed the protected health information of its patients to third parties including Facebook and Google.

20. Under G.L. c. 214, § 1B, all persons "have a right against unreasonable, substantial, or serious interference" with their privacy.

21. Medical patients such as Jane Doe have a legal interest in preserving the confidentiality of their communications with healthcare providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

22. Patients also have reasonable expectations of privacy that their personal identifiable information and protected health information (together "PII/PHI") and communications will not be disclosed to third parties without their express written consent and authorization.

23. As a health care provider, Defendant has ethical, fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

24. Defendant expressly and impliedly promises patients that it will maintain and protect the confidentiality of PII/PHI and communications.

25. Defendant operates websites for patients, including:

- www.capecodhealth.org;
- <https://www.capecodhealth.org/locations/profile/cape-cod-hospital/>;
- <https://www.capecodhealth.org/locations/profile/falmouth-hospital/>; and
- <https://www.capecodhealth.org/locations/profile/jml-care-center/>.

26. Defendant's websites are designed for interactive communication with patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues treatment options, and joining support groups.

27. Defendant encourages patients to use digital tools on its websites to seek and receive health care services.

28. The home pages of Defendant's websites are designed for use by patients. The homepage provides patients with tools to seek medical treatment, such as finding a doctor, researching services and treatments, and paying bills.

29. Defendant also maintains a patient portal, which allows patients to make appointments, access medical records, view lab results, and exchange communications with health care providers.

30. Notwithstanding patients' reasonable expectations of privacy, Defendant's legal duties of confidentiality, and Defendant's express promises to the contrary, Defendant discloses the contents of patients' communications and protected healthcare information via automatic routing mechanisms embedded in the website operated by Defendant without patients' knowledge, authorization, or consent.

C. Defendant misuses sophisticated software to automatically collect and disclose patient PII/PHI to third-party advertising companies like Google and Facebook.

31. Defendant's disclosures of patients' personal healthcare information occur because Defendant intentionally deploys source code on the websites it operates, including www.capecodhealth.org, that causes patients' personally identifiable information (including the exact contents of their communications) to be transmitted to third parties.

32. By design, third parties receive and record the exact contents of patient communications before the full response from Defendant to patients has been rendered on the screen of the patient's computer device and while the communication between Defendant and the patient remains ongoing.

33. For example, when Plaintiffs or a Class Member accessed Defendant's website pages hosting the Meta Pixel, the Meta Pixel software directed their browsers to send a message to Facebook's servers. The information that Defendant sent to Facebook included the private information that Plaintiffs and Class Members communicated to Defendant's website, such as the type of medical appointment the patient made, the date, and the specific doctor the patient was seeing. Such private information allows third-party advertising companies like Facebook to determine that a specific patient was seeking a specific type of confidential medical treatment. This kind of disclosure also allows Facebook to reasonably infer that a specific patient was being treated for specific types of medical conditions, such as cancer and pregnancy.

34. Websites like those maintained by Defendant are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users via their web browsers.

35. Web browsers are software applications that allow users to exchange electronic communications over the internet.

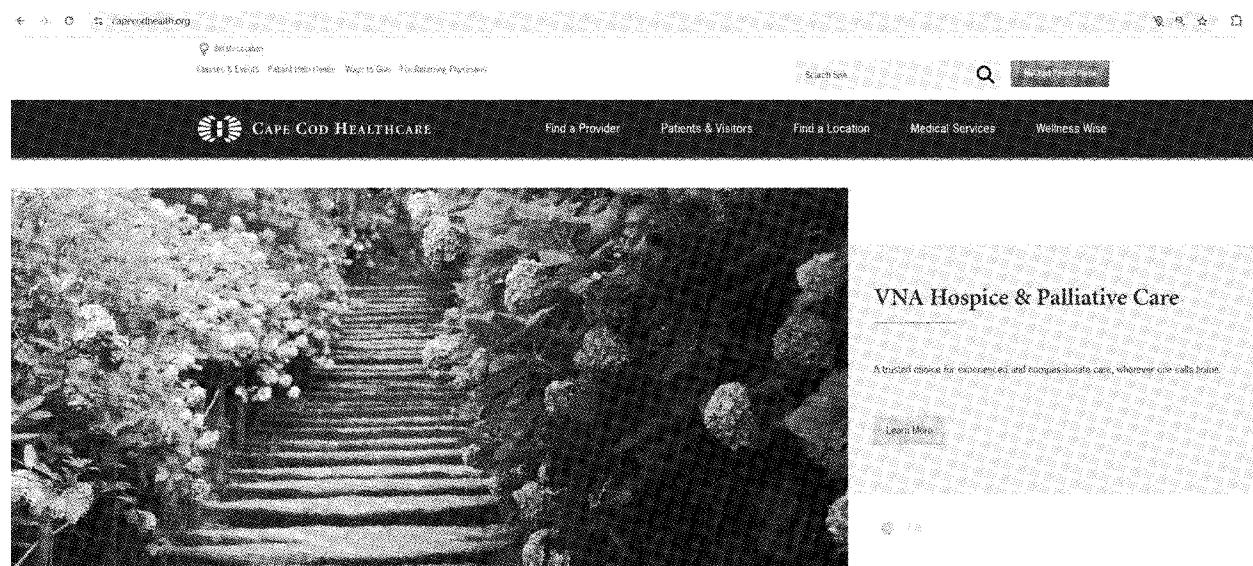
36. Each exchange of an electronic communication over the internet typically consists of an HTTP request from a client device and an HTTP response from a server. When a user types

a URL into a web browser, for example, the URL is sent as an HTTP request to the server corresponding to the web address, and the server then returns an HTTP response that consists of a web page to display in the client device's web browser.

37. In addition to specifying the URL, HTTP requests can also send data to the host server, including users' cookies. Cookies are text files stored on client devices to record data, often containing sensitive, personally identifiable information.

38. In turn, HTTP responses may consist, among other things, of a web page, another kind of file, text information, or error codes. A web page consists primarily of "Markup" and "Source Code." The markup of a web page comprises the visible portion of that web page. Markup is displayed by a web browser in the form of words, paragraphs, images, and videos displayed on a users' device screen. A web page's source code is a set of instructions that commands browsers to take certain actions, either when the web page loads or when a specified event triggers the code.

39. For example, typing <https://www.capecodhealth.org> into a browser sends an HTTP request to Cape Cod Healthcare's website, which returns a HTTP response in the form of the home page of Cape Cod Healthcare's website:



40. Source code is not visible on the user device’s screen, but it may change the markup of a webpage, thereby changing what is displayed on the user device’s screen. Source code may also execute a host of other programmatic instructions, including commanding a web browser to send data transmissions in the form of HTTP requests to the website’s server, or as is the case with Defendants’ website, to third parties via pixels.

41. For example, Cape Cod Healthcare’s website has included software code that transmits HTTP requests directly to Facebook, including patients’ PII/PHI, every time a patient interacts with a page on its website.

42. The basic command that web browsers use to exchange data and user communications is called a GET request.⁷ For example, when a patient types “heart failure treatment” into the search box on Defendant’s website and hits ‘Enter,’ the patient’s web browser makes a connection with the server for Defendant’s website and sends the following request: “GET search/q=heart+failure+treatment.”

43. When a server receives a GET request, the information becomes appended to the next URL (or “Uniform Resource Locator”) accessed by the user. For example, if a user enters “respiratory problems” into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words “respiratory” and “problems” will be appended to the query string at the end of the URL of the webpage showing the search results.

44. The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks ‘Enter’ or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

⁷ https://www.w3schools.com/tags/ref_httpmethods.asp

45. In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website's responsive communication.

46. Unbeknownst to users, however, the website's server may also redirect the user's communications to third parties, like Facebook and Google. Indeed, Google warns website developers and publishers that installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.⁸ Typically, users are provided no notice that these disclosures are being made.

47. Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

48. In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

49. These tracking pixels can collect dozens of data points about individual website users who interact with a website.

50. For example, one of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

51. Tracking pixels such as the Meta Pixel tool allow Defendant and Facebook to secretly track, intercept, record, and transmit every patient communication made on Defendant's websites. When patients visit Defendant's websites, unbeknownst to them, the web page displayed on the patient's browser includes the Meta Pixel as embedded code, which is not visible to patients or other visitors to Defendant's websites. This code is triggered when a patient

⁸ <https://support.google.com/platformspolicy/answer/6156630?hl=en>

or visitor interacts with the web page. Each time the Meta Pixel is triggered, the software code is executed and sends patient's PII/PHI directly to Facebook.

52. The Meta Pixel and similar tracking pixels act like a physical wiretap on a phone. Like a physical wiretap, pixels do not appear to alter the function of the communication device on which they surreptitiously installed. Instead, these pixels lie in wait until they are triggered by an event, at which time they effectively open a channel through the website to funnel data about users and their actions to third parties via a hidden HTTP request that is never shown to or agreed to by the user.

53. For example, a patient can trigger an HTTP request by interacting with the search bar on Defendants' websites by typing a term such as "breast cancer" into the search bar and then hitting enter. Defendants' servers in turn send an HTTP response, which results in the search results being displayed.

54. This is not the only HTTP request, however, that is created by a patient's interaction with Defendant's website. In fact, at the very same time the web page is instructed to send an HTTP request to Defendant requesting search results, the embedded source code, acting as a tap, is triggered, such that Defendant's websites are also instructed to send an HTTP request directly to Facebook, Google, and other third parties informing them of the patient's exact search and the patient's identifiable information.

55. In addition to employing the Meta Pixel to track patients, Defendant's web properties and patient portal used Google Analytics, to track and disclose patient activity—including Plaintiffs'—without their consent. Unbeknownst, the installation of this code inside patient portal resulted in disclosures of patients' personal health information, including their patient status, whenever they logged into the patient portal for routine purposes such as reviewing medical records, checking lab results, and communicating with their doctors. The

Google Analytics pixel within the patient portal also disclosed when patients viewed specific pages within the patient portal, including prescription information and test results.

56. In addition, through Google Analytics, Defendant disclosed Plaintiffs' activity by tracking and disclosing their IP addresses, cookies, geolocation, and other unique device identifiers. Defendant routinely disclosed patients' PII/PHI to Google using this technology.

57. A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website for every third party they wish to send user data and communications.

58. Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

59. Tag managers are simple enough that non-programmers can use them to deploy and remove digital tracking tools from web-properties with just the click of a few buttons.

60. Defendant deployed Google Tag Manager on its websites through an "iframe," a nested "frame" that exists within the Defendant's website that is, in reality, an invisible window through which Defendant funneled tracking pixels for third parties to secretly acquire the content of patient communications without any knowledge, consent, authorization, or further action of patients.

61. By design, none of the tracking was visible to patients visiting Defendant's websites.

D. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website.

62. Tracking pixels are particularly pernicious because they result in the disclosure of a variety of data that permits third parties to determine the unique personal identities of website visitors. While most users believe that the internet provides them with anonymity when, for

example, they browse a hospital website for treatment information about a medical condition, that is not the case when the hospital website has embedded third party tracking devices, as Defendant has.

63. For example, an IP address is a numerical identifier that identifies each computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices—one that has limited privacy controls.⁹

64. Because of their uniquely identifying character, IP addresses are considered protected personally identifiable information by HIPAA. *See 45 C.F.R. § 164.514(b)(2)(i)(O).* Tracking pixels can (and typically do) collect website visitors' IP addresses.

65. Likewise, internet cookies also provide personally identifiable information. Cookies are small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Cookies are typically designed to acquire and record an individual internet user's communications and activities on websites and were developed by programmers to aid with online advertising.

66. Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

⁹ <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>

67. Cookies fall within the personal identifiers protected by HIPAA (*see* 45 C.F.R. § 164.51(b)(2)(i)(H), (J), (M), and (R)), and tracking pixels can collect cookies from website visitors.

68. In general, cookies are categorized by (1) duration and (2) party.

69. There are two types of cookies classified by duration.

70. “Session cookies” are placed on a user’s computing device only while the user is navigating the website that placed and accesses the cookie. The user’s web browser typically deletes session cookies when the user closes the browser.

71. “Persistent cookies” are designed to survive beyond a single internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user’s internet communications for years and over dozens or even hundreds of websites. Persistent cookies are also called “tracking cookies.”

72. Cookies are also classified by the party that uses the collected data.

73. “First-party cookies” are set on a user’s device by the website with which the user is exchanging communications. First-party cookies can be helpful to the user, server, and/or website to assist with security, login, and functionality.

74. “Third-party cookies” are set on a user’s device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits Defendants’ websites will also have cookies on their device from third parties, such as Facebook and Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

75. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire

and record user data and communications in order to sell advertising that is customized to a user's communications and habits. To build individual profiles of internet users, third party data companies assign each user a unique identifier or set of unique identifiers.

76. Traditionally, first party and third-party cookies were kept separate. An internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Defendant can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record a patient's communications, Defendant is not permitted direct access to Facebook third-party cookie values. The reverse *was* also true: Facebook was not provided direct access to the values associated with first-party cookies set by companies like Defendant. But data companies have designed a way to hack around the same-origin policy so that third-party data companies like Facebook can gain access to first-party cookies.

77. JavaScript source code developed by third party data companies and placed on a webpage by developers such as Defendant can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as "cookie synching," and it allows two cooperating websites to learn each other's cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information that they have collected and recorded about a user that is associated with a cookie identifier number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

78. In effect, cookie synching is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set for first-party

websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking. On information and belief, the letters fbp are an acronym for Facebook Pixel.

79. The Facebook _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the health care provider using the Meta Pixel.

80. The _fbp cookie is also a third-party cookie in that it is also a cookie associated with Facebook that is used by Facebook to associate information about a person and their communications with non-Facebook entities while the person is on a non-Facebook website or app.

81. Defendant requires patients using its patient portal to have enabled first-party cookies to gain access to its patient portal.

82. The _fbp cookie is used as a unique identifier for patients by Facebook.

83. If a patient takes an action to delete or clear third-party cookies from their device, the _fbp cookie is not impacted—even though it is a Facebook cookie—because Facebook has disguised it as a first-party cookie. Facebook also uses IP addresses and user-agent information to match the health information it receives from Defendant with Facebook users.

84. Defendant has engaged in cookie synching with Facebook, Google, and other third parties.

85. Defendant's cookie disclosures include the deployment of cookie synching techniques that cause the disclosure of the first-party cookie values that Defendant assigns to patients to also be made to third parties.

86. Defendant has used and caused the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

87. A third type of personally identifying information is what data companies refer to as a “browser-fingerprint.” A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

88. These browser-fingerprints can be used to uniquely identify individual users when a computing device’s IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, “With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites.”¹⁰ The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.¹¹ Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.¹²

89. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.¹³

90. Browser-fingerprints are considered protected personal identifiers under HIPAA (*see* 45 C.F.R. § 164.514(b)(2)(i)(M), (R)), and tracking pixels can collect browser-fingerprints from website visitors.

91. Defendant has used and caused the disclosure of data sufficient for third parties to create a browser-fingerprint identifier with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

92. A fourth kind of personally identifying information is the unique user identifier (such as Facebook’s “Facebook ID”) that permits companies like Facebook to quickly and

¹⁰ <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹¹ <https://pixelprivacy.com/resources/browser-fingerprinting/>

¹² <https://www.blog.google/products/chrome/building-a-more-private-web/>

¹³ <https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/>

automatically identify the personal identity of its user across the internet whenever the identifier is encountered. A Facebook ID is a number string that is connected to a user's Facebook profile.¹⁴ Anyone with access to a user's Facebook ID can locate a user's Facebook profile.¹⁵

93. Unique personal identifiers such as a person's Facebook ID are protected by HIPAA (*see* 45 C.F.R. § 164.514(b)(2)(i)(M), (R)) and are likewise capable of collection through pixel trackers.

94. Each of the individual data elements described above is personally identifiable on their own. However, Defendant's disclosures of such personally identifiable data elements do not occur in a vacuum. The disclosures of the different data elements are tied together and, when taken together, these data elements are even more accurate in identifying individual patients, particularly when disclosed to data companies such as Facebook, Google, and other internet marketing companies that expressly state that they use such data elements to identify individuals.

E. Facebook's Business Model: Exploiting Users' Personal Information for Profit.

95. Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

96. Facebook describes itself as a "real identity" platform.¹⁶ This means that users are permitted only one account and must share "the name they go by in everyday life."¹⁷ To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.¹⁸

97. In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver

¹⁴ <https://www.facebook.com/help/211813265517027>

¹⁵ <https://smallseotools.com/find-facebook-id/>

¹⁶ <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.>

¹⁷ <https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/>

¹⁸ <https://www.facebook.com/help/406644739431633>

more tailored and relevant ads.”¹⁹ Facebook has since evolved into one of the largest advertising companies in the world.²⁰ Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.²¹ This allows Facebook to make inferences about users based on their interests, behavior, and connections.²²

98. Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.²³

99. Facebook maintains profiles on users that include users’ real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users’ habits and interests.

100. Tracking information about users’ habits and interests is a critical component of Facebook’s business model because it is precisely this kind of information that allows Facebook to sell advertising to its customers. Facebook uses plug-ins and cookies to track users’ browsing histories when they visit third-party websites. Facebook then compiles these browsing histories into personal profiles which are sold to advertisers to generate profits.

101. Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting “Core Audiences,” “Custom Audiences,” “Look Alike Audiences,” and even more granulated approaches within audiences

¹⁹ <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>

²⁰ <https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/>

²¹ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

²² <https://www.facebook.com/business/ads/ad-targeting>

²³ <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

called “Detailed Targeting.” Each of Facebook’s advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

102. Ad Targeting has been extremely successful due to Facebook’s ability to target individuals at a granular level. For example, among many possible target audiences, “Facebook offers advertisers 1.5 million people ‘whose activity on Facebook suggests that they’re more likely to engage with/distribute liberal political content’ and nearly seven million Facebook users who ‘prefer high-value goods in Mexico.’”²⁴ Aided by highly granular data used to target specific users, Facebook’s advertising segment quickly became Facebook’s most successful business unit, with millions of companies and individuals utilizing Facebook’s advertising services.

103. Defendant knew or should have known that Facebook could not be trusted with its patients’ sensitive medical information given its history of violating consumers’ privacy through unauthorized use of their personal information in general, and for marketing purposes, specifically.

104. Despite knowing that the Meta Pixel code embedded in its websites was sending patients’ PII/PHI to Facebook, Defendant did nothing to protect its patients from egregious intrusions into its patients’ privacy, choosing instead to benefit at those patients’ expense.

105. Additionally, there is widespread knowledge within the health care community that installation of the Meta Pixel tool on hospital websites results in the disclosure of patients’ PII/PHI to Facebook, as evidenced by multiple data breaches experienced by hospitals where

²⁴ <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>

data gathered by the Meta Pixel code was stolen by cybercriminals. There is also widespread recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy rights involved.

F. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

106. To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its “Like” and “Share” buttons (known as “social plug-ins”), and other methodologies, which it then uses to power its advertising business.

107. One of Facebook’s most powerful tools is called the “Meta Pixel.”

108. The Meta Pixel is a snippet of code embedded on a third-party website that tracks users’ activities as users navigate through a website.²⁵ Once activated, the Meta Pixel “tracks the people and type of actions they take.”²⁶ Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.²⁷ The Meta Pixel code works by sending Facebook a detailed log of a user’s interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website or how far down a web page they scrolled.²⁸

109. When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.²⁹

²⁵ <https://developers.facebook.com/docs/meta-pixel/>

²⁶ <https://www.facebook.com/business/goals/retargeting>

²⁷ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

²⁸ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

²⁹ See, e.g., *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).

110. The transmission is instantaneous—indeed Facebook often receives the information before the health care provider does.

111. The transmission is invisible.

112. The transmission is made without any affirmative action taken by the patient.

113. The information Meta Pixel captures and discloses to Facebook includes a referrer header (or “URL”), which includes significant information regarding the user’s browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.³⁰ When users enter a URL address into their web browser using the ‘http’ web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user’s browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

114. These search terms and the resulting URLs divulge a user’s personal interests, queries, and habits on third-party websites operating outside of Facebook’s own platform. In this manner, Facebook tracks users browsing histories on third-party websites, and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.³¹

115. For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook also receives personally identifying information like IP addresses, Facebook IDs, and other data that allow Facebook to identify the user. All this personally identifying data is available each time the Meta Pixel forwards a user’s interactions with a third-party website to Facebook’s servers. Once

³⁰ *In re Facebook*, 956 F.3d at 596.

³¹ *In re Facebook*, 956 F.3d at 596.

Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

116. These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.³²

117. The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.³³

118. In exchange for installing its Meta Pixel, Facebook provides website owners like Defendant with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.³⁴ The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.³⁵

119. Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

120. Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."³⁶ According to Facebook, the Meta Pixel is an analytics tool that

³² <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

³³ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

³⁴ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

³⁵ <https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector>

³⁶ <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/>

allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites.”³⁷

121. Facebook warns web developers that its Pixel is a personal identifier because it enables Facebook “to match your website visitors to their respective Facebook User accounts.”³⁸

122. Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website’s persistent header) to reduce the chance of browsers or code from blocking Pixel’s execution and to ensure that visitors will be tracked.³⁹

123. Once Meta Pixel is installed on a business’s website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including PII/PHI), as well as “optional values” set by the business website.⁴⁰ Facebook builds user profiles on users that include the user’s real name, address, location, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, such as IP addresses and the Facebook ID. Meta Pixel tracks this data regardless of whether a user is logged into Facebook.⁴¹

124. Facebook tracks non-Facebook users through its widespread internet marketing products and source code and Mark Zuckerberg has conceded that the company maintains “shadow profiles” on nonusers of Facebook.⁴²

125. For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user’s internet browser, similar to how a “bug” or wiretap can capture audio information.

126. For example, the Meta Pixel is configured to automatically collect “HTTP

³⁷ <https://www.oviond.com/understanding-the-facebook-pixel>

³⁸ <https://developers.facebook.com/docs/meta-pixel/get-started>

³⁹ <https://developers.facebook.com/docs/meta-pixel/get-started>

⁴⁰ <https://developers.facebook.com/docs/meta-pixel/>

⁴¹ <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>

⁴² <https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/>

Headers" and "Pixel-specific data."⁴³ HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."⁴⁴ Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."⁴⁵

127. Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID, which identifies an individual's Facebook user account. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.⁴⁶

128. Facebook also receives personally identifying information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's unique IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

129. Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

130. The data supplied by the c_user cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type www.facebook.com/#, with the c_user identifier in place of the "#." For example, the c_user

⁴³ <https://developers.facebook.com/docs/meta-pixel/>

⁴⁴ <https://developers.facebook.com/docs/meta-pixel/>

⁴⁵ <https://developers.facebook.com/docs/meta-pixel/>

⁴⁶ <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

cookie for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

131. Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as "datr," "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.⁴⁷ These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.⁴⁸

132. Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like www.emersonhospital.org and target users with advertising based on their web activity.

133. Facebook then sells advertising space by highlighting its ability to target users. Facebook can target users so effectively because it surveils user activity both on and off its official website. This allows Facebook to make inferences about users far beyond what they

⁴⁷ <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbd8a#:~:text=browser%20session%20ends.-,%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.>

⁴⁸ https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

explicitly disclose, like their “interests,” “behavior,” and “connections.”⁴⁹ Facebook compiles this information into a generalized dataset called “Core Audiences,” which advertisers use to create highly specific targeted advertising. Indeed, Facebook utilizes precisely the type of PII/PHI that Defendant bartered to Facebook so that Facebook can identify, target, and market products and services to individuals.

G. Defendant has discretely embedded the Meta Pixel tool on its website, capturing and disclosing patients’ PII/PHI to Facebook.

134. A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user’s experience and activity on the website to assess the website’s functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

135. Facebook’s intrusion into the personal data of visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.⁵⁰ Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

136. Facebook provides websites using Meta Pixel with the data it captures in the “Meta Pixel page” in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.⁵¹ For example, websites can use this data to create “custom

⁴⁹ <https://www.facebook.com/business/ads/ad-targeting>

⁵⁰ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

⁵¹ <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>

audiences” to target the specific Facebook user, as well as other Facebook users who match “custom audience’s” criteria.⁵² Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

137. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.⁵³ Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for advertising purposes.⁵⁴

138. For example, when a user on many of these hospital websites clicks on a “Schedule Online” button next to a doctor’s name, Meta Pixel sends the text of the button, the doctor’s name, and the search term (such as “cardiology”) used to find the doctor to Facebook. If the hospital’s website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

139. Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, to create an appointment—Facebook code embedded on that page redirects the content of the patient’s communications to Facebook while the exchange of information between the patient and hospital is still occurring.

140. Defendant is among the hospital systems who have embedded Meta Pixel on their websites.

141. When a patient entered their personal information through Defendant’s websites that incorporate Meta Pixel, including to locate a doctor or make an appointment, this information, including what the patient is being treated for, those communications are

⁵² <https://developers.facebook.com/docs/marketing-api/reference/custom-audience/>

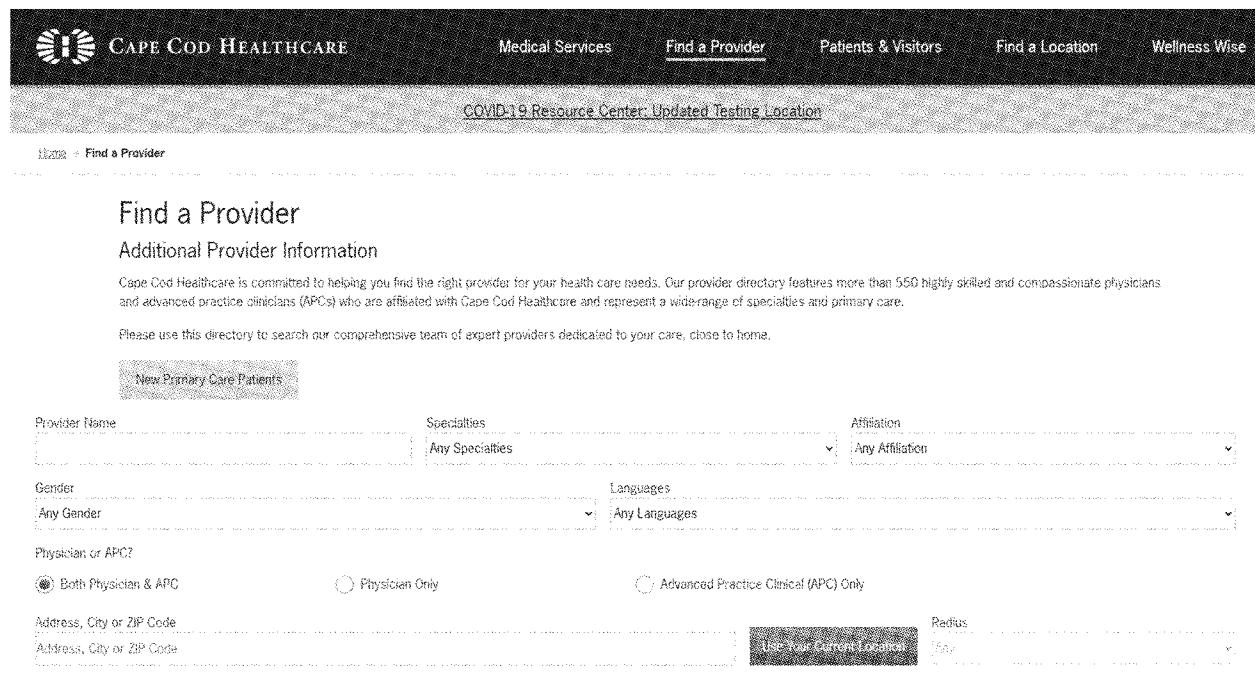
⁵³ <https://instapage.com/blog/meta-pixel>

⁵⁴ <https://instapage.com/blog/meta-pixel>

immediately and instantaneously routed to Facebook via the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

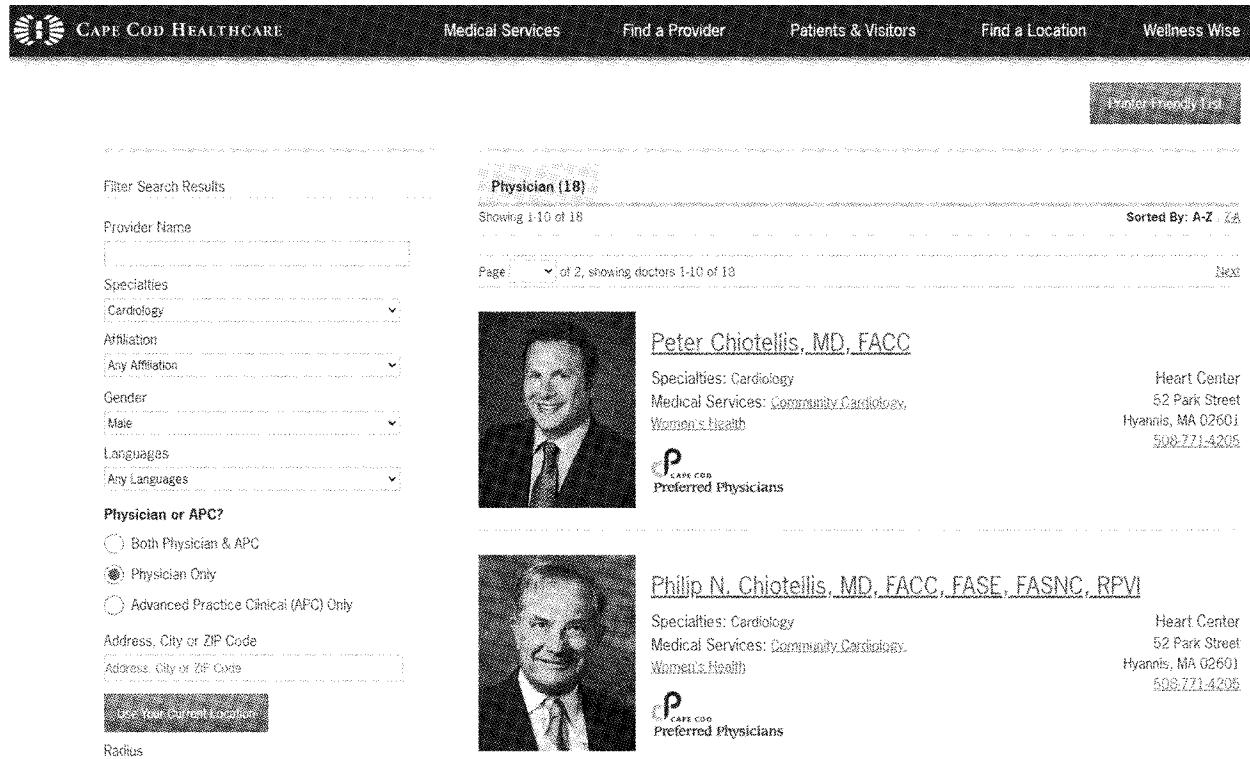
142. This data, which can include health conditions (e.g., addiction, Alzheimer's, heart disease), diagnoses, procedures, test results, the treating physician, medications, and other PII/PHI is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising.

143. For example, a patient searching for a doctor on Defendant's website is asked to provide a variety of information to filter the various physicians available to treat various medical conditions, including the doctor's specialty, the patient's condition, the patient's hometown, the patient's language preference, and other information that the patient provides.



The screenshot shows the Cape Cod Healthcare website's provider search interface. At the top, there is a navigation bar with links for Medical Services, Find a Provider (which is underlined in blue), Patients & Visitors, Find a Location, and Wellness Wise. Below the navigation bar, a banner for the COVID-19 Resource Center and Updated Testing Location is visible. The main content area is titled "Find a Provider" and includes a sub-section for "Additional Provider Information". It features several dropdown menus and input fields for filtering providers by name, specialty, language, affiliation, gender, and practice type (Both Physician & APC, Physician Only, Advanced Practice Clinical (APC) Only). There are also fields for entering an address or ZIP code and a radius selection. A "Use Your Current Location" button is present.

144. The search criteria entered by prospective patients then results in the website providing a list of potential treating physicians who can provide the requested medical services:



Filter Search Results

Provider Name

Specialties

Cardiology

Affiliation

Any Affiliation

Gender

Male

Languages

Any Languages

Physician or APC?

Both Physician & APC

Physician Only

Advanced Practice Clinical (APC) Only

Address, City or ZIP Code

Radius

Medical Services

Find a Provider

Patients & Visitors

Find a Location

Wellness Wise

Print Friendly List

Physician (18)

Showing 1-10 of 18

Sorted By: A-Z

Peter Chiotellis, MD, FACC

Specialties: Cardiology
Medical Services: Community Cardiology, Women's Health

Heart Center
52 Park Street
Hyannis, MA 02601
508.771.4205

 Preferred Physicians

Philip N. Chiotellis, MD, FACC, FASE, FASNC, RPVI

Specialties: Cardiology
Medical Services: Community Cardiology, Women's Health

Heart Center
52 Park Street
Hyannis, MA 02601
508.771.4205

 Preferred Physicians

145. All this data was disclosed to Facebook simultaneously in real time via the Meta Pixel as patients transmit their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also disclosed other personally identifying information to Facebook, such as patient IP addresses, cookie identifiers, browser-fingerprints, and device identifiers.

146. Defendant disclosed such personally identifying information and sensitive medical information even when patients were searching for doctors to assist them with conditions such as substance abuse and addiction:

 CAPE COD HEALTHCARE

Medical Services Find a Provider Patients & Visitors

COVID-19 Resource Center: Updated Testing Location

[Home](#) > Site Search

Site Search

substance abuse

Search

Related Pages

Found 107 pages matching the search term **substance abuse**.

- [\\$22 million in healthcare, one resident at a time](#)
8/23/2015
Community Benefits programs extend outreach to the Cape's most vulnerable and hard-to-reach populations.
- [Brian Elyon's 18th overdose was his last](#)
11/5/2015
A mother grieves the death of her son—and the critical need to help those battling drug addiction on the Cape.
- [Red Cross honors Cape Cod Hospital innovators](#)
4/3/2017
The maternity and pediatric departments will be recognized for work with substance-exposed newborns and their moms.
- [Cape Cod Healthcare Designates Up to \\$2.5 million to Address Substance Use Disorders](#)
1/13/2017
Cape Cod Healthcare has designated up to \$2.5 million to prevent and treat substance use disorder in the community.

147. Likewise, a patient who searches the website for information about receiving certain specific forms of medical treatment such as orthopedics, heart & vascular care, or cancer care also has information about their queries and the specific web pages that the patient has visited acquired by Defendant and forwarded to Facebook:

 CAPE COD HEALTHCARE

Medical Services Find a Provider Patients & Visitors Find a Location Wellness Wise

COVID-19 Resource Center: Updated Testing Location

Cancer Care

Edward J. Vayda, DO - Oncology (Medical)

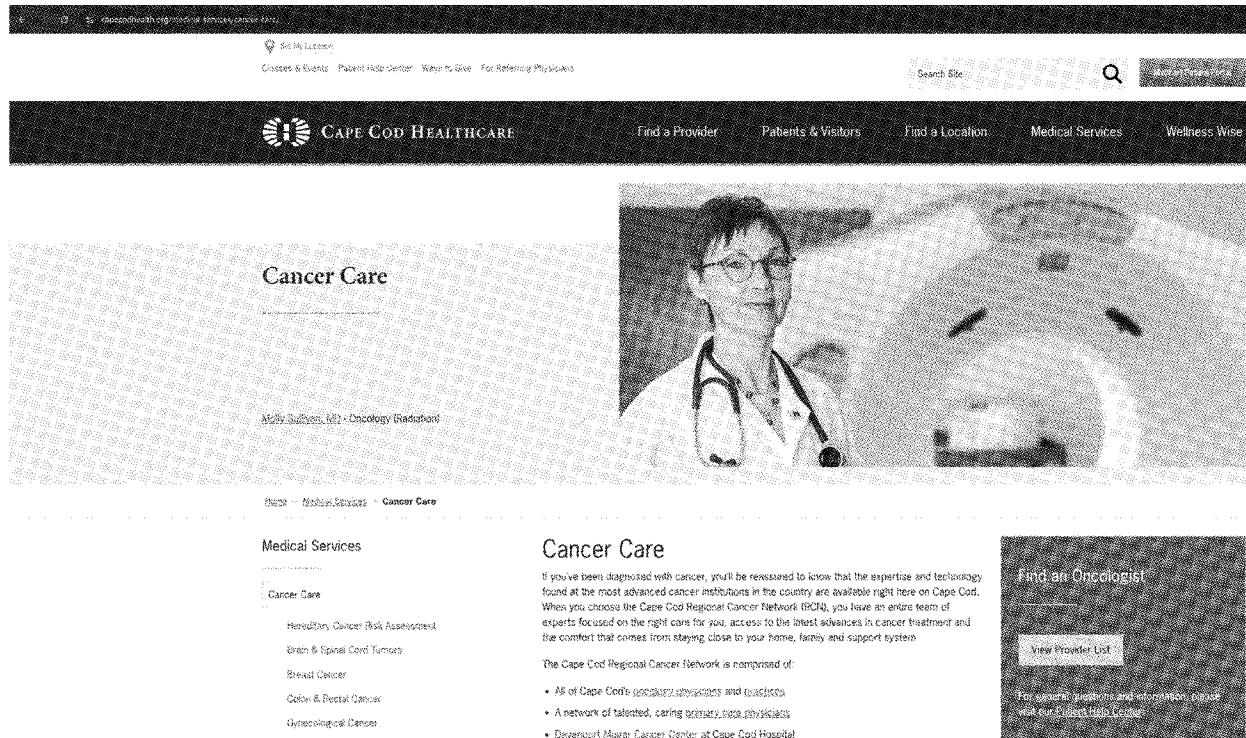


Home > Medical Services > Cancer Care

148. Defendant also disclosed patient information from other sections of its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for "Medical Services" offered by Defendant, communications made by patients using the website's Bill Pay/Financials function, and communications made when patients are researching specific medical conditions such as COVID-19.

149. Defendant made similar disclosures to Facebook, Google, and other third parties when patients click on the "Log in" buttons of the password protected portions of its website, including its patient portal and bill pay functions, confirming to these companies that the website users are Cape Cod Health patients. For example, Defendant allows patients to search for information about "Medical Services," such as "Allergy & Immunology," "Behavioral Health," "Cancer Care," and "Pregnancy & Birth."⁵⁵ A patient searching for information about cancer treatment or pregnancy, however, not only shares their personal data with Defendant but also unknowingly shares their personal data with Facebook such as the fact that they have cancer:

⁵⁵ <https://www.capecodhealth.org/medical-services/>



150. Defendant has disclosed patient PII/PHI collected across their websites including (but not limited to) the following communications:

- when patients search via Defendant's search bars for their required care (e.g., for "substance abuse");
- when patients search for a physician or provider—which reveal their location and required medical services and medical conditions (e.g., searching for "Gynecology");
- when patients search for, register for, and/or click on classes or events;
- when patients research treatment information and medical services; and
- when patients select "Locations" and then enter their ZIP code, the medical service they are seeking (e.g., "Behavioral Health"), and required location type (e.g., "Hospital").

151. In other words, Facebook learned not just that patients are seeking treatment, but where and typically when they are seeking treatment, along with other information that patients would reasonably assume that Defendant is not sharing with third party marketing companies.

152. Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

153. The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Defendant's websites. The path identifies where a file can be found on a website. Likewise, a query string provides a list of parameters. The query string parameters in this search indicate that a search was done at Defendant's website for information about HIV. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider and that patient's specific healthcare issue.

154. Defendant also provided Facebook with details about online forms that patients fill out in the form of POST requests. All the information that patients provided when filling out these forms was also disclosed to Facebook.

155. As the above demonstrates, knowing what information a patient is reviewing on Defendant's websites can reveal deeply personal and private information. For example, a simple search for "pregnancy" on Defendant's websites tells Facebook that the patient is likely pregnant. Indeed, Facebook might know that the patient is pregnant before the patient's close

family and friends. But there is nothing visible on Defendant's websites that would indicate to patients that, when they used Defendant's search function, their personally identifiable data and the precise content of their communications with Defendant was being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

156. The amount of data collected is significant. Via the Meta Pixel, when patients interacted with its website, Defendant disclosed a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient typed a search term into the search bar on Defendant's websites, the website returns linked to information relevant to the search term. When patients then clicked these links, a communication is created that contains a GET request and a full-string detailed URL.

157. By compelling visitors to its websites to disclose personally identifying data and sensitive medical information to Facebook and other third parties, Defendant knowingly discloses information that allows Facebook and other advertisers to link its patients' Personal Health Information to their private identities and target them with advertising. Defendant intentionally shares the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

158. The contents of patients' search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Defendant's website. Worse, no matter how sensitive the area of the Defendant's website that a patient reviewed, the referral URL was acquired by Facebook along with other PII/PHI.

159. The nature of the collected data is also important. Defendant's unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient's medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Defendant's website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

160. Defendant also disclosed the same kind of patient data described above to other third parties involved in internet marketing, including Google, via tracking software that Defendant has installed on its websites. As with the Facebook Meta Pixel, Defendant has provided patients and prospective patients with no notice that Defendant was disclosing the contents of their communications to these third parties. Likewise, Defendant has not obtained consent from patients and prospective patients before forwarding their communications to these companies.

161. These disclosures to third parties other than Facebook are equally disturbing. Google Analytics, for example, has been described by the Wall Street Journal as "far and away the web's most dominant analytics platform," which "tracks you whether or not you are logged in."⁵⁶ Like Facebook, Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers. Defendant routinely disclosed patients' PII/PHI to such Google services as Google Analytics.

162. Google cookies provided personally identifiable data about patients who visit Defendant's websites to Google. Defendant transmitted personally identifiable Google cookie data to Google.

163. Google warns web-developers that Google marketing tools are not appropriate for health-related webpages and websites. Indeed, Google warns web developers that "Health" is a

⁵⁶ <https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401>

prohibited category that should not be used by advertisers to target ads to users or promote advertisers' products or services.

164. Defendant deployed Google tracking tools on nearly every page of its websites, resulting in the disclosure of communications exchanged with patients to be transmitted to Google. Defendant even deployed these tools inside of its password protected patient portal through Google Tag Manager. These transmissions occur simultaneously with patients' communications with Defendant and include communications that Plaintiffs and Class Members made about specific medical providers, treatments, conditions, appointments, payments, and registrations and logins to Defendant's patient portals.

165. By compelling visitors to its websites to disclose personally identifiable data and sensitive medical information to Facebook, Defendant knowingly discloses information that allows Facebook and other advertisers to link their patients' PII/PHI to their private identities and target them with advertising (or do whatever else Facebook may choose to do with their information, including running "experiments" on its customers by manipulating the information they are shown on their Facebook pages).⁵⁷ Defendant intentionally shares the PII/PHI of their patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

166. The information Plaintiffs and Class Members provide to Cape Cod Health via its website (and then shared illegally with Facebook) can be combined with other information in Facebook's possession, like their names, dates of birth, and phone numbers, to more effectively target Plaintiffs with advertisements or sell Plaintiffs' data to third parties.

167. Because Defendant embedded the Meta Pixel on their websites, Defendant disclosed intimate details about Plaintiffs' interactions with the websites, including Plaintiffs' scrolling, typing, and selecting options from drop down menus. Each time the Meta Pixel was

⁵⁷ <https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>

triggered, it caused Plaintiffs' information to be secretly transmitted to Facebook's servers, as well as additional information that captures and discloses the communications' content and Plaintiffs' identities. For example, when Plaintiffs and Class Members visited Defendant's websites, their PII/PHI was transmitted to Facebook, including such engagement as using the website's search bar, using the website's "Find a Doctor" function, and typing content into online forms. During these same transmissions, Defendant's websites would also provide Facebook with Plaintiffs' and Class Members' Facebook ID, IP addresses, device IDs, and other information that Plaintiffs and Class Members provided. This is precisely the type of information that state and federal law require healthcare providers to de-identify to protect the privacy of patients.

168. Defendant knew that by embedding Meta Pixel—a Facebook advertising tool—it was permitting Facebook to collect, use, and share Plaintiffs' and the Class Members' PII/PHI, including sensitive medical information and personally identifiable data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant made the decision to barter its patients' PII/PHI to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it betrayed the rights of Plaintiffs and Class Members.

H. Plaintiffs and the Class Members did not consent to the interception and disclosure of their protected health information.

169. Plaintiffs and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is seamlessly integrated into Defendant's websites and is invisible to patients visiting those websites.

170. For example, when Plaintiffs visited Defendant's website at

www.capecodhealth.org, there was no indication that Meta Pixel or other tracking technologies were embedded on that website or that it would collect and transmit their sensitive medical data to Facebook.

171. Plaintiffs and their fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

172. While Defendant purports to have a "Privacy Policy," that Privacy Policy is effectively hidden from patients. Unlike most hospital websites, the home page of Defendant's website contains no link to its online Privacy Policy.⁵⁸ Instead, the only way that a visitor to Defendant's website could even locate the Privacy Policy is by entering the term "Privacy" or something similar in the website's search bar and engaging the search function.

173. Defendant's "Privacy Policy" gives no indication to patients that Defendant routinely allows Facebook to capture and exploit patients' Personal Health Information. Indeed, Defendant expressly promises in its "Privacy Policy" that it would safeguard both the identities and the personal health information provided by visitors to its website⁵⁹:

Privacy Policy

Cape Cod Healthcare's Internet Privacy Policy

At Cape Cod Healthcare, we are committed to protecting the privacy and security of the users of our Internet site. We understand that one's health is often a very personal, private subject, and, accordingly, we are committed to protecting the identities of visitors to our site. This Privacy Policy will tell you what information we collect, how it is used, and what your choices are. Please read this policy carefully.

This statement is false, deceptive, and misleading because Defendant in fact tracks patients' and potential patients' IP addresses, cookies, browser-fingerprints, and device identifiers, which it then causes the transmission of the same to third parties along with patients' and potential patients' sensitive medical information.

⁵⁸ <https://www.capecodhealth.org/>

⁵⁹ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

174. Even if a patient stumbled upon Defendant's carefully hidden "Privacy Policy," nothing in that notice would be understood by any reasonable patient to mean that Defendant is routinely allowing Facebook to capture and exploit patients' Personal Health Information.

175. While disclosing that its website contains "cookies," Defendant's Privacy Policy falsely promises that the information Defendant collects "do not contain any personally identifiable information."⁶⁰ Contrary to that promise, Defendant's website automatically transmits personally identifiable information to Facebook using multiple cookies, including the c_user, datr, fr, sb, and xs cookies.

176. Defendant does not have a legal right to share Plaintiffs' and Class Members' Protected Health Information with Facebook, because this information is protected from such disclosure by law. *See* G.L. c. 214, §1B; 45 C.F.R. § 164.508. Moreover, Defendant is not permitted to disclose patients' Personal Health Information to an advertising and marketing company like Facebook without express written authorization from patients. *Id.*

177. Defendant failed to obtain a valid written authorization from Plaintiffs or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

178. A patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Such "Browser-Wrap" statements do not create an enforceable contract against consumers. Further, Defendant expressly promised its patients that it would never sell or use their Personal Health Information for marketing purposes without express authorization.

179. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiffs and Class Members' PII/PHI to Facebook or aid in the same.

⁶⁰ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

I. The disclosures of personal patient data to Facebook are unnecessary.

180. There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are any of the disclosures of patient PII/PHI to Facebook or Google necessary for Defendant to maintain its healthcare website or provide medical services to patients.

181. For example, it is possible for a healthcare website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Defendant to provide medical services to patients without sharing their Personal Health Information with Facebook so that this information can be exploited for advertising purposes.

182. Indeed, after Plaintiffs filed suit in October 2022, Defendant removed the Facebook Meta Pixel from all pages on its website.

183. Despite the wholly unnecessary nature of the Meta Pixel for Defendant to run its business, Defendant willfully chose to implement Meta Pixel and other tracking technologies on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third-parties, including Facebook.

J. Plaintiffs and Class Members have a reasonable expectation of privacy in their PII/PHI, especially with respect to sensitive medical information.

184. Patient confidentiality "is a cardinal rule of the medical profession, faithfully adhered to in most instances, and thus has come to be justifiably relied upon by patients seeking advice and treatment." *Alberts v. Devine*, 395 Mass. 59, 65 (1985).

185. As patients, Plaintiffs and Class Members had a reasonable expectation of privacy that their healthcare provider would not disclose their PII/PHI to third parties without their express authorization. Defendant's surreptitious interception, collection, and disclosure of patients' Personal Health Information to Facebook violated Plaintiffs and Class Member's privacy interests.

186. Patient Personal Health Information is specifically protected by law. *E.g.* G.L. 111, §70E(b); G.L. 214, §1B (Right to Privacy). The prohibitions against disclosing patients' Personal Health Information include prohibitions against disclosing personally identifying data such as patient names, IP addresses, and other unique characteristics or codes. *See* G.L. c. 111, § 70E (Patients' and Residents' Rights); 105 Mass. Code Regs. 300.120; 45 C.F.R. § 164.514(b)(2)(i). And both HIPAA and Massachusetts law subject medical providers who treat conditions such as substance abuse to heightened duties of confidentiality. 42 C.F.R. § 2.12(a)(1)(i); M.G.L. c. 111B, § 11. This legal framework applies to health care providers, such as Defendant.

187. Moreover, the modern Hippocratic Oath provides, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."⁶¹ Likewise, the American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications. For example, the AMA has issued medical ethics opinions providing that "[p]rotecting information gathered in association with the care of a patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust Physicians must seek to protect patient privacy in all settings to the greatest extent possible and should ... [m]inimize intrusion on privacy when the patient's privacy must be balanced against other factors [and inform] the patient when there has been a significant infringement on

⁶¹ https://www.pbs.org/wgbh/nova/doctors/oath_modern.html

privacy of which the patient would otherwise not be aware.”⁶²

188. The AMA’s ethics opinions have further cautioned physicians and hospitals that “[d]isclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship.”⁶³

189. Several studies examining the collection and disclosure of consumers’ sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

190. Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual’s affirmative consent before a company collects and shares its customers’ data.

191. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers’ data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.⁶⁴

192. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.⁶⁵

193. The concern about sharing personal medical information is compounded by the

⁶² <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (opinion 3.1.1).

⁶³ <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf> (opinion 3.2.4).

⁶⁴ <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/>

⁶⁵ <https://www.wired.co.uk/article/apple-ios14-facebook>

reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, “What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children’s data and have the potential to store a plurality of data traces under unique ID profiles.”⁶⁶

194. Many privacy law experts have expressed serious concerns about patients’ sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient’s personal health information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

K. Defendant harmed Plaintiffs when it illicitly collected, disclosed, and exploited Plaintiffs’ PII/PHI—which, after all, is Plaintiffs’ property, and has economic value.

195. It is common knowledge that there is an economic market for consumers’ personal data—including the kind of data that Defendant has collected and disclosed from Plaintiffs and Class Members.

196. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, “age, gender and location information” were being sold for approximately “\$0.50 per 1,000 people.”⁶⁷

197. In 2015, *TechCrunch* reported that “to obtain a list containing the names of individuals suffering from a particular disease,” a market participant would have to spend about “\$0.30” per name.⁶⁸ That same article noted that “Data has become a strategic asset that allows

⁶⁶ <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>

⁶⁷ <https://ig.ft.com/how-much-is-your-personal-data-worth/>

⁶⁸ <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

companies to acquire or maintain a competitive edge” and that the value of a single user’s data can vary from \$15 to more than \$40 per user.⁶⁹

198. In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers “should think of Facebook’s cost as [their] data and scrutinize the power it has to set its own price.”⁷⁰ This price is only increasing. According to Facebook’s own financial statements, the value of the average American’s data in advertising sales rose from \$19 to \$164 per year between 2013 and 2020.⁷¹

199. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.⁷²

200. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,⁷³ and has paid teenagers and adults up to \$20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.⁷⁴

201. A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.⁷⁵

202. Given the monetary value that data companies like Facebook have already paid

⁶⁹ <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>

⁷⁰ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

⁷¹ <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/>

⁷² <https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/>; *see also* <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>

⁷³ <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app>

⁷⁴ <https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>

⁷⁵ <https://www.creditdonkey.com/best-apps-data-collection.html>; *see also* <https://www.monetha.io/blog/rewards/earn-money-from-your-data/>

for personal information in the past, Defendant has deprived Plaintiffs and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiffs and the Class Member's property.

L. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of its patients' PII/PHI.

203. In exchange for disclosing PII/PHI about its patients, Defendant has been compensated by Facebook with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions.

204. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

205. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

206. Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Defendant loses the ability to control how that information is subsequently disseminated and exploited.

207. The monetization of the data being disclosed by Defendant, both by Defendant and Facebook, demonstrates the inherent value of the information being collected.

TOLLING, CONCEALMENT, AND ESTOPPEL

208. The applicable statutes of limitation have been tolled as a result of Defendant's

knowing and active concealment and denial of the facts alleged herein.

209. Defendant seamlessly incorporated Meta Pixel, Google Analytics, and other tracking pixels into its websites, providing no indication to users that they were interacting with a website enabled by such tracking technologies. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with its websites that Plaintiffs and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

210. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

211. The earliest that Plaintiffs and Class Members, acting with due diligence, could have reasonably discovered this conduct would have been on June 16, 2022, following the release of the Markup's investigation.

212. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of patients' Personal Health Information has continued unabated through the date of the filing of Plaintiffs' Original Complaint. What's more, Defendant was under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

213. Defendant's conduct violates the law and breaches its express and implied privacy promises.

214. Defendant's unlawful conduct has injured Plaintiffs and Class Members.

215. Defendant's conduct is ongoing.

216. Plaintiffs brings this action individually and as a class action against Defendant.

217. Plaintiffs seek class certification for the following proposed Class:

The Massachusetts Class: During the fullest period allowed by law, all current Massachusetts citizens who are, or were, patients of Cape Cod Healthcare or any of its affiliates and who exchanged communications at Cape Cod Healthcare's websites, including www.capecodhealth.org and any other Cape Cod Healthcare hospital affiliated website.

The Nationwide Class: During the fullest period allowed by law, all current or former patients of Cape Cod Healthcare or any of its affiliates who exchanged communications at Cape Cod Healthcare's websites, including www.capecodhealth.org and any other Cape Cod Healthcare, Inc. affiliated website.

218. Excluded from the proposed Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and Defendant's counsel.

219. Plaintiffs reserve the right to redefine the Classes and/or add Subclasses at, or prior to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

220. This action is properly maintainable as a class action as specifically defined in Massachusetts Rule of Civil Procedure 23.

221. **Numerosity:** While the exact number of Class Members is unknown to Plaintiffs at this time, the Classes, based on information and belief, consist of thousands of people such that joinder of all members is impracticable. The exact number of Class Members can be determined by review of information maintained by Defendants.

222. **Commonality and Predominance:** There are questions of law and fact common to Class Members and which predominate over any questions affecting only individual members.

A class action will generate common answers to the questions below, which are apt to drive resolution:

- a. Whether Defendant's acts and practices violated Plaintiffs and Class Members' privacy rights;
- b. Whether Defendant's acts and practices violate 18 U.S.C § 2510, et seq.;
- c. Whether Defendant's acts and practices violate G.L. c. 214, § 1B;
- d. Whether Defendant's acts and practices violate G.L. c. 111, § 70E;
- e. Whether Defendant knowingly allowed the surreptitious collection and disclosure of Plaintiffs and Class Members' PII/PHI to Facebook and other third parties;
- f. Whether Defendant's acts and practices constitute a breach of fiduciary duty;
- g. Whether Defendant profited from disclosures of PII/PHI to third parties including Facebook;
- h. Whether Defendant was unjustly enriched;
- i. Whether Defendant's acts and practices harmed and continue to harm Plaintiffs and Class Members and, if so, the extent of that injury;
- j. Whether Plaintiffs and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and
- k. Whether Plaintiffs and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

223. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

224. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

225. **Typicality:** Plaintiffs' claims are typical of the claims of other Class Members and Plaintiffs have substantially the same interest in this matter as other Class Members.

Plaintiffs has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiffs' claims arise out of the same set of facts and conduct as all other Class Members. Plaintiffs and all Class Members are patients of Defendant who used the websites set up by Defendant for patients and are victims of Defendant's respective unauthorized disclosures to third parties including Facebook. All claims of Plaintiffs and Class Members are based on Defendant's wrongful conduct and unauthorized disclosures.

226. Adequacy of Representation: Plaintiffs are committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiffs' claims are coincident with, and not antagonistic to, those of other Class Members they seeks to represent. Plaintiffs have no disabling conflicts with Class Members. Accordingly, Plaintiffs are an adequate representative of the Class and, along with counsel, will fairly and adequately protect the interests of the Class and any Subclasses.

227. Superiority: A class action is the superior method for fair and efficient adjudication of the controversy. Although all Class Members have claims against Defendant, the likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation. The damages, harm, and other detriment suffered individually by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impractical for Class Members to individually seek redress for Defendant's wrongful conduct. Moreover, serial adjudication in numerous venues is not efficient, timely, or proper. Judicial resources would be unnecessarily depleted by prosecution of individual claims. The prosecution of separate actions by individual Class Members could create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which could establish incompatible standards of conduct for Defendant or adjudications with respect to

individual members of the Class which would, as a practical matter, be dispositive of the interests of the members of the Class Members who are not parties to the adjudications. If a class action is not permitted, Class Members will continue to suffer losses and Defendant's misconduct will continue without proper remedy.

228. Plaintiffs anticipate no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable, and direct notice can be provided from the records maintained by Defendant, electronically or by publication, the cost of which is properly imposed on Defendant.

229. For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action.

CAUSES OF ACTION

COUNT I

Interception of Wire Communications in Violation of 18 U.S.C. § 2510, *et seq.* (On Behalf of Plaintiffs and the Nationwide Class)

230. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

231. The Electronic Communications Privacy Act (the "ECPA"), 18 U.S.C. § 2510, protects individuals against eavesdropping committed with an improper purpose.

232. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119 of Title 18 of the United States Code.

233. A violation of Chapter 119 and the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or

having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

234. Plaintiffs' communications with Defendant on its web properties and patient portal are covered communications under 18 U.S.C. §§ 2510, 2511.

235. Plaintiffs' and Class Members' communications with Defendant constitute "electronic communications" because each communication was the transfer of data or intelligence, including, but not limited to:

- a. the parties to the communications;
- b. the precise text of patient search queries;
- c. personally identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;
- d. the precise text of patient communications about specific doctors;
- e. the precise text of patient communications about specific medical conditions;
- f. the precise text of patient communications about specific treatments;
- g. the precise text of patient communications about scheduling appointments with medical providers;
- h. the precise text of patient communications about billing and payment;
- i. the precise text of specific buttons on Defendant's website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

- j. the precise dates and times when patients click to Log-In on Defendant's website(s);
- k. The precise dates and times when patients visit Defendant's websites;
- l. information that is a general summary or informs third parties of the general subject of communications that Defendant sent back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and
- m. any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

236. Plaintiffs and Class Members's communications with Defendant constitute "electronic communications" because they were wholly or partially transmitted by wire, electromagnetic, and/or photoelectronic systems including but not limited to:

- a. Plaintiffs and Class Members' personal computing devices;
- b. Plaintiffs and Class Members' web browsers;
- c. Plaintiffs and Class Members' browser-managed files;
- d. Facebook's Meta Pixel;
- e. Internet cookies;
- f. Defendant's computer servers; and
- g. Third-party source code used by Defendants.

237. Whenever Plaintiffs and Patient Class members interacted with Defendant's web properties, including their MyChart patient portal, Defendant, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally divulged the contents of Plaintiffs and Class members' electronic communications while those

communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

238. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

239. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

240. Thus, although Defendant is a "part[y] to the communications" at issue, it still incurs liability under the ECPA because it captured and redirected Plaintiffs' information to third parties without consent and for criminal and tortious purposes, as alleged throughout this complaint.

241. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Massachusetts including, among other things:

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Invasion of privacy in violation of G.L. c. 214, § 1B;
- c. Breach of confidentiality of medical records in violation of G.L. c. 111, § 70E; and
- d. Breach of the common law duty of confidentiality.

242. For example, under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person ... without authorization" from the patient.

243. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

244. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

245. Defendant accessed, obtained, and disclosed Plaintiffs’ and Class Members’ Personal Health Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

246. As such, Defendant cannot viably claim any exception to ECPA liability.

247. As a result, Defendant harmed Plaintiffs and the Class, breaching the confidentiality of their medical information, violating their privacy, breaching their contract with the hospital, depriving them the full benefit of their bargain with Defendant for care, and causing actual damages in an amount to be proven at trial.

248. The ECPA provides that persons whose electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119 may recover statutory damages of the greater of \$100 a day for each day of violation or \$10,000. 18 U.S.C. § 2520.

249. For these reasons, Plaintiffs, individually and on behalf of the Class members, seeks all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys’ fees and costs.

COUNT II
Invasion of Privacy in Violation of G.L. c. 214, § 1B
(On Behalf of Plaintiffs and the Massachusetts Class)

250. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

251. Plaintiffs bring this claim on behalf of themselves and all members of the Class.

252. G.L. c. 214, § 1B provides that “a person shall have a right against unreasonable, substantial, or serious interference with her privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.”

253. All health care providers owe their patients a duty not to disclose medical information about a patient without a patient’s informed consent.

254. G.L. c. 111, § 70E provides that every patient or resident of a Massachusetts health care facility shall have the right to “confidentiality of all records and communications to the extent provided by law.”

255. Maintaining the confidentiality of the doctor-patient relationship is a cardinal rule of the medical profession which has come to be justifiably relied on by patients seeking advice and treatments.

256. Plaintiffs and Class Members are patients of Defendant.

257. Defendant owes Plaintiffs and Class Members a duty of confidentiality.

258. Despite its duty not to disclose Personal Health Information without informed consent and written authorization, Defendant disclosed information relating to Plaintiffs and Class Members’ medical treatment to third parties without their knowledge, consent, or authorization.

259. The information disclosed included personally identifiable information, Plaintiffs and Class Members’ statuses as patients of Defendant, and the exact contents of communications exchanged between Plaintiffs and/or Class Members with Defendant, including but not limited to

information about treating doctors, potential doctors, conditions, treatments, appointments, search terms, bill payment, and logins to Defendant's website.

260. The disclosure of personally identifiable medical information constitutes an unreasonable, substantial, and serious interference with Plaintiffs and Class Members' rights to privacy.

261. Plaintiffs and Class Members did not consent to, authorize, or know about Defendant's disclosure of their Personal Health Information to Facebook and other third parties at the time it occurred. Plaintiffs and Class Members never agreed that their sensitive medical information could be collected, used, and monetized by Facebook.

262. Defendant's intentional disclosure of patients' Personal Health Information to a third-party advertising company like Facebook without consent would be highly offensive to a reasonable person. Plaintiffs and Class Members reasonably expected that their Personal Health Information would not be collected, used, and monetized by third party advertising companies.

263. Defendant's disclosure of Personal Health Information from thousands of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that Americans believe that one of the most important privacy rights is the need for an individual's affirmative consent before their personal data is collected, shared, or used.

264. Given the nature of the Personal Health Information that Defendant disclosed to Facebook, such as patients' names, email addresses, phone numbers, information entered into forms, doctor's names, potential doctor's names, the search terms used to locate doctors (i.e. "Alzheimer's"), the condition selected from dropdown menus (i.e. "Heart Disease"), medications, and details about upcoming doctor's appointments, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

265. Defendant's breach caused Plaintiffs and Class Members, at minimum, the following damages:

- a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- b. Defendant eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;
- d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain the confidentiality of their Personal Health Information; and
- e. Defendant's actions diminished the value of Plaintiffs and Class Members' personal information.

266. Plaintiffs and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights.

267. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to seek just compensation, including monetary damages.

268. Plaintiffs and Class Members seek appropriate relief for their injuries, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as well as a disgorgement of profits made by Defendant as a result of its intrusions on Plaintiffs and Class Members' privacy.

269. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, which caused injury to Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

270. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III
Breach of Fiduciary Duty and/or Common Law Duty of Confidentiality
(On Behalf of Plaintiffs and the Massachusetts Class)

271. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

272. Plaintiffs bring this claim on behalf of themselves and all members of the Class.

273. All conditions precedent to this action have been performed or occurred.

274. In *Alberts v. Devine*, 479 N.E.2d 113, 120 (1985), the Massachusetts Supreme Court held that a duty of confidentiality arises from the physician-patient relationship and that a violation of that duty gives rise to a cause of action sounding in tort.

275. As medical provider for Plaintiffs and Class Members, Defendant owes Plaintiffs and Class Members a fiduciary duty of confidentiality in the data and content of communications exchanged between Defendant and Plaintiffs or Class Members.

276. Defendant breached its duty of confidentiality by disclosing Personal Health Information about Plaintiffs and Class Members, including their status as patients, the content of their communications, and information about their doctors, potential doctors, conditions, treatments, appointments, search terms, and bill payment.

277. Defendant's breach caused Plaintiffs and Class Members the following damages:

- a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- b. Defendant eroded the essential confidential nature of the doctor-patient and provider-patient relationship;
- c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs and Class Members' knowledge, consent, or authorization and without sharing the benefit of such value;
- d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain the confidentiality of their Personal Health Information; and
- e. Defendant's actions diminished the value of Plaintiffs and Class Members' personal information.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Massachusetts Class)

278. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

279. Plaintiffs bring this claim on behalf of themselves and all members of the Class.

280. Defendant promises in its Privacy Policy that it is committed to protecting patients' sensitive medical and personal information, telling patients that "we are committed to protecting the privacy and security of the users of our Internet site."⁷⁶ Defendant assures patients that the information it collects about patients does not include any "personally identifiable information."⁷⁷ Defendant also promises that "Cape Cod Healthcare wants your personal information to remain as secure as possible. Accordingly, we prevent unauthorized access by a

⁷⁶ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

⁷⁷ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

secure firewall and through our use of a security infrastructure to protect the integrity and privacy of the personal information you provide to us.”⁷⁸

281. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Health Information on its website as part of Defendant’s regular business practices. Plaintiffs and Class Members accepted Defendant’s offers and provided their Private Health Information to Defendant as part of acquiring Defendant’s medical services. Per its contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate measures to protect Plaintiffs’ and Class Members’ Personal Health Information from unauthorized disclosure to third parties such as Facebook. These facts give rise to the inference that Defendant took on obligations outside the plain terms of any express contracts that they may have had with Plaintiffs and Class Members.

282. Plaintiffs and the Class Members entered into valid and enforceable implied contracts with Defendant when they sought medical treatment from Defendant. Specifically, through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for the provision of medical care and treatment, which included an implied agreement for Defendant to retain and protect the privacy of Plaintiffs’ and Class Members’ Personal Health Information.

283. Defendant required and obtained Plaintiffs’ and Class Members’ Personal Health Information as part of the physician-patient relationship, evincing an implicit promise by Defendant to act reasonably to protect the confidentiality of Plaintiffs’ and Class Members’ Personal Health Information. Defendant, through its privacy policies, codes of conduct, company security practices, and other conduct, implicitly that it would safeguard Plaintiffs’ and Class Members’ Personal Health Information in exchange for access to that information and the opportunity to treat Plaintiffs and Class Members.

⁷⁸ <https://www.capecodhealth.org/about/policies-notices/privacy-policy/>

284. Implied in the exchange was a promise by Defendant to ensure that the Personal Health Information of Plaintiffs and Class Members in its possession would only be used for medical treatment purposes and would not be shared with third parties such as Facebook without the knowledge or consent of Plaintiffs and Class Members. By asking for and obtaining Plaintiffs' and Class Members' Personal Health Information, Defendant assented to protecting the confidentiality of that information. Defendant's implicit agreement to safeguard the confidentiality of Plaintiffs' and Class Members' Personal Health Information was necessary to effectuate the contract between the parties.

285. Plaintiffs and Class Members provided their Personal Health Information in reliance on Defendant's implied promise that this information would be safeguarded and not disclosed to third parties without their consent.

286. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class Members would provide their Personal Health Information in exchange for the medical treatment and other benefits provided by Defendant (including the protection of their confidential personal and medical information). A portion of the price of each payment that Plaintiffs and the Class Members made to Defendant for medical services was intended to ensure the confidentiality of their Personal Health Information.

287. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant would comply with its promises to protect the confidentiality of their Personal Health Information as well as applicable laws and regulations governing the disclosure of such information and that Defendant would not allow third parties to collect or exploit their communications with Defendant without their consent.

288. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiffs and Class Members would not have disclosed their

Personal Health Information to Defendant but for the prospect of Defendant's promise of medical treatment and other benefits. Conversely, Defendant presumably would not have taken Plaintiffs and Class Members' Personal Health Information if it did not intend to provide them with medical treatment and other benefits.

289. Defendant was therefore required to reasonably safeguard and protect the Personal Health Information of Plaintiffs and Class Members from unauthorized disclosure and/or use by third parties.

290. Plaintiffs and Class Members accepted Defendant's medical services offer and fully performed their obligations under the implied contract with Defendant by providing their Personal Health Information to Defendant among other obligations. Plaintiffs and Class Members would not have provided and entrusted their Personal Health Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Personal Health Information for uses other than the benefits offered by Defendant.

291. Plaintiffs and Class Members relied on Defendant's implied promises to safeguard their Personal Health Information to their detriment. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Personal Health Information from disclosure to Facebook and other third parties.

292. Defendant's failure to implement adequate measures to protect the Personal Health Information of Plaintiffs and Class Members and Defendant's intentional disclosure of the same to Facebook violated the purpose of the agreement between the parties: Plaintiffs' and Class Members' provision of money and Personal Health Information in exchange for medical services and other benefits.

293. Instead of safeguarding Plaintiffs' and Class Members' Personal Health Information, Defendant intentionally shared that information with Facebook thereby breaching the implied contracts it had with Plaintiffs and Class Members.

294. Plaintiffs and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so. Plaintiffs and Class Members would not have purchased medical services from Defendant if they knew that Defendant would share their Personal Health Information with Facebook without their knowledge or written consent.

295. Plaintiffs and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to operate its websites free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so.

296. Under the implied contracts, Defendant and/or its affiliated healthcare providers promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' Personal Health Information provided to obtain such healthcare. In exchange, Plaintiffs and Class Members agreed to pay money for these services, and to turn over their Personal Health Information through the use of Defendant's websites.

297. Both the provision of medical services healthcare and the protection of Plaintiffs and Class Members' Private Health Information were material aspects of these implied contracts.

298. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Health Information unless they consent—are also acknowledged, memorialized, and

embodied in multiple documents, including (among other documents) Defendant's published Notice of Privacy Practices.

299. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorialize and embody an implied contractual obligation requiring Defendant refrain from aiding or allowing third parties to collect or Plaintiffs and Class Members' Private Health Information without consent. By soliciting and acquiring Plaintiffs' and Class Members' Personal Health Information, Defendant assumed an independent duty to handle Plaintiffs' and Class Members' Personal Health Information with due care and consistent with industry standards to prevent the foreseeable harm that arises from a breach of that duty.

300. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Health Information associated with obtaining healthcare private. To customers such as Plaintiffs and the Class Members, healthcare that allows third parties to secretly collect their Private Health Information without consent is fundamentally less useful and less valuable than healthcare that refrains from such practices. Plaintiffs and Class Members would not have entrusted their Private Health Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Health Information would be safeguarded and protected or entrusted their Private Health Information to Defendant in the absence of its implied promise to do so.

301. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their Private Health Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, (a) the provision of healthcare and medical services and (b) the protection of their Private Health Information.

302. Plaintiffs and the Class Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Health Information.

303. Defendant materially breached its contractual obligation to protect the nonpublic Private Health Information Defendant gathered when it allowed third parties to collect and exploit that information without Plaintiffs and Class Members' consent.

304. Defendant also materially breached its contractual obligation to protect Plaintiffs' and Class Members' non-public Personal Health Information when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant (1) failed to implement internal policies and procedures prohibiting the disclosure of patients' Personal Health Information without consent to third-party advertising companies like Facebook, (2) failed to implement adequate reviews of the software code and java script installed on its websites to ensure that patients' Personal Health Information was not being automatically routed without consent to third party advertising companies like Facebook, (3) failed to provide adequate notice to the public that visitors to its websites risked having their Personal Health Information shared with third party advertising companies like Facebook, (4) failed to take other industry standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages, (5) failed to provide visitors to its websites with a means to opt out of the automatic transfer of data regarding their website interactions to third party advertising companies like Facebook, (6) failed to implement internal policies and educational programs to ensure that Defendants' website managers and coders were familiar with the legal regulations governing the disclosure patient Personal Health Information to third parties, and (7) failed to install adequate firewalls or take similar measures to prevent the automatic routing of patients' Personal Health Information to third party advertising companies like Facebook.

305. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to those described in the contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the healthcare services with data privacy they paid for and the healthcare services they received.

306. As a result of Defendant's material breaches, Plaintiffs and Class Members were deprived of the benefit of their bargain with Defendant because they spent more on medical services with Defendant than they would have if they had known that Defendant was not providing the reasonable data security and confidentiality of patient communications that Defendant represented that it was providing in its privacy policies. Defendant's failure to honor its promises that it would protect the confidentiality of patient communications thus resulted in Plaintiffs and Class Members overpaying Defendant for the services they received.

307. The services that Plaintiffs and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

308. The medical services that Defendant offers are available from many other health care systems who do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiffs' and Class Members' Private Health Information without consent, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

309. Defendant's conduct in sharing Plaintiffs' and Class Members' Personal Health Information with Facebook also diminished the sales value of that information. There is a robust market for the type of information that Plaintiffs and Class Members shared with Defendant (which Defendant then shared with Facebook). Indeed, Facebook itself has offered to pay the public to acquire similar information in the past so that Facebook could use such information for marketing purposes. Plaintiffs and Class Members were harmed both by the dissemination of their Personal Health Information and by losing the sales value of that information.

310. As a direct and proximate result of these failures, Plaintiffs and the Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Private Health Information, the loss of control of their Private Health Information, the diminution in value of their Personal Health Information, and the loss of the benefit of the bargain they had struck with Defendant.

311. Plaintiffs and the Class Members are entitled to compensatory and consequential damages suffered as a result.

312. Plaintiffs and Class Members also face a real and immediate threat of future injury to the confidentiality of their Personal Health information both because such information remains within Defendant's control and because anytime that Plaintiffs and/or Class Members interact with Defendant's websites to make appointments, such information about their medical conditions, search for a doctor, or otherwise seek assistance with their medical conditions they risk further disclosure of their Personal Health Information. Plaintiffs and the Class Members are therefore also entitled to injunctive relief requiring Defendant to cease all website operations that allow for the third-party capture of Private Health Information.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Massachusetts Class)

313. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

314. Plaintiffs hereby plead this Count in the alternative to Count IV.

315. Plaintiffs bring this claim on behalf of themselves and all members of the Massachusetts Class.

316. Plaintiffs and Class Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiffs and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

317. Plaintiffs and the Class Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

318. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

319. The benefits that Defendant derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

320. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, ask for judgment in their favor, and that the Court enter an order as follows:

- a. Certifying the Classes and appointing Plaintiffs as the Classes' representatives;
- b. Appoint the law firms of Sweeny Merrigan Law, Keller Postman LLC, and Ahmad, Zavitsanos, & Mensing P.C. as class counsel;
- c. Finding that Defendant's conduct as alleged herein was unlawful;
- d. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Defendant from making any further disclosure of Plaintiffs or Class Members' communications to third parties without the Plaintiffs or Class Members' express, informed, and written consent;
- e. Awarding statutory damages of \$10,000 per Plaintiffs and Class Members pursuant to 18 U.S.C. § 2520;
- f. Imposing a constructive trust against Defendant through which Plaintiffs and Class Members can be compensated for any unjust enrichment gained by Defendant;
- g. Awarding damages for violations of Plaintiffs and Class Members' right to privacy;
- h. Awarding Plaintiffs and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- i. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law;
- j. Awarding Plaintiffs and Class Members reasonable attorney's fees, costs, and expenses;

- k. Awarding costs of suit; and
- l. Such other and further relief to which Plaintiffs and Class Members may be entitled.

Respectfully submitted,

/s/ Jonathan T. Merrigan

J. Tucker Merrigan, BBO# 681627
Ryan Hawkins, BBO# 686289
Erin E. McHugh, BBO# 703701
Sweeney Merrigan Law
268 Summer St. LL
Boston, MA 02210
Tel: (617) 391-9001
Fax: (617) 357-9001
tucker@sweeneymerrigan.com
rmh@sweeneymerrigan.com
emchugh@sweeneymerrigan.com

Foster C. Johnson (*pro hac vice*)
David Warden (*pro hac vice*)
Justin C. Kenney (*pro hac vice*)
Nathan Campbell (*pro hac vice*)
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston, Texas 77010
(713) 655-1101
fjohnson@azalaw.com
dwarden@azalaw.com
jkenney@azalaw.com
ncampbell@azalaw.com

Alex Dravillas (*pro hac vice*)
Keller Postman LLC
150 N. Riverside Plaza
Suite 4100
Chicago, Illinois 60606
(312) 741-5220
adj@kellerpostman.com

**COUNSEL FOR PLAINTIFFS,
INDIVIDUALLY AND ON BEHALF OF ALL
OTHERS SIMILARLY SITUATED**